

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011 covering the prior calendar year 2010

Date filed: February 28, 2011

Name of company(s) covered by this certification: Name of company(s) covered by this certification:
Broadpoint, LLC and its wholly-owned subsidiary Broadpoint License Co., LLC (collectively, "the
Company")

Form 499 Filer ID: 825542

Name of signatory: Bryan Olivier

Title of signatory: Chief Operating Officer

I, Bryan Olivier, certify that I am an officer of the Company, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

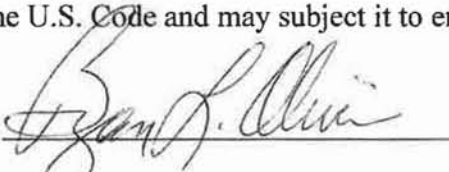
Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The Company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17, which requires truthful and accurate statements to the Commission. The Company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed



Attachment: Accompanying Statement Explaining CPNI Procedures

Broadpoint, LLC and its wholly-owned subsidiary Broadpoint License Co., LLC Explanation of Compliance with FCC CPNI Rules

To ensure compliance with Federal Communications Commission ("FCC" or "Commission") rules and orders governing protection, use, and disclosure of customer proprietary network information ("CPNI"), Broadpoint, LLC and its wholly-owned subsidiary Broadpoint License Co., LLC (collectively, "the Company") have adopted the attached CPNI Policy and Employee Guidelines ("CPNI Policy"). An officer of the company has been assigned responsibility for ensuring that the CPNI Policy is consistently followed, that CPNI complaints and problem reports are appropriately responded to, and that all required reports to law enforcement and the FCC are timely made. All employees that have access to customers or customer data are made aware of the CPNI Policy through review of the policy and its requirements. A copy of the CPNI Policy has been provided to each such employee.



Safeguarding Customer Proprietary Network Information Company Policy and Employee Guidelines

Policy Statement: It is the policy of the Company to protect and maintain the confidentiality of customer proprietary network information as required by federal law. The Company has a duty under federal law to protect the confidentiality of customer information and relies on its employees to fulfill that duty. Customer proprietary network information will be used or disclosed by Company employees only in accord with applicable federal regulations and Company procedures as described below.

Types of customer information protected: During the course of a customer's relationship with the Company, the Company will come into possession of information about the customer's use of the Company's services. Federal law specifically protects customer information that relates to the quantity, technical configuration, type, destination, location, and amount of use of the customer's service, as well as any telephone service information contained in the customer's bill.¹ Such information may include, for example, the phone numbers called by a customer, the length of the calls, and records of additional services purchased by the customer, such as voice mail.

Restrictions on use and disclosure of customer information: Customer information may not be used by or disclosed to anyone outside of the Company without the customer's permission. This includes Company affiliates, unless the customer is also a customer of that affiliate. Within the Company, customer information may not be used to market services in any category of services to which the customer does not currently subscribe, unless the customer has given permission. Categories of service for purposes of this restriction are local exchange service, long-distance service, and wireless service.

Types of Customer Permission Required: Different types of customer permission are required for different types of customer information use or disclosure. Upon written request from the customer, the customer's information may be disclosed to any person designated by the customer. Customers seeking to access their customer information on-line must produce a password previously set by the customer.

Customers seeking to access their information by telephone must produce a password² to obtain release over the phone of call detail information.³ A customer who has lost or forgotten his or

¹ These types of information have been termed "customer proprietary network information" or "CPNI" by the Federal Communications Commission.

² The requirement to produce a password does not apply to business customers where: (a) the customer's contract is serviced by a dedicated account representative as the primary contact; (b) the contract specifically addresses the protection of customer information; and (c) the business customer is not required to go through a call center to reach a customer service representative.

³ Call detail information is any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or

her password may be authenticated by correctly answering one or more questions established with the Company at the time the password was set up. Customer information (other than call detail) may be given to the customer over the phone without a password once the customer satisfies the Company employee of his or her identity. Customers may, over the phone without producing a password, request that the Company send call detail information to the customer's postal or e-mail address of record or request that the Company call the customer's telephone number of record with the requested call detail.

Customer permission required for the Company use of customer information in various types of marketing is described further below.

Exceptions to use and disclosure restrictions: The law allows the Company to use or disclose customer information without permission for the following purposes:

1. to provide services (including installation, maintenance, repair, and billing for services) in any category of services to which the customer subscribes;
2. to market services (including marketing upgrades to basic service) in any category of services to which the customer already subscribes;
3. to protect the Company, its customers, or other parties against fraudulent, abusive or unlawful use of services; or
4. to respond to a legal demand for the information (e.g., a subpoena or court order).

Supervisors may authorize employee use of customer information for purposes #1 and #2, above. Use of customer information for purpose #2 must follow guidelines described below. Supervisors faced with a situation described in purposes #3 and #4 should consult with the Company's counsel before using or disclosing any customer information. Questions about any of these situations, or demands for use of customer information other than those described above should be directed to the Company's counsel.

Customer permission to use or disclose customer information for marketing campaigns: The Company may seek permission from customers to use their customer information in marketing campaigns for other categories of services than those to which the customer currently subscribes. Once customer permission has been obtained, customer information may be used by the Company and its affiliates to market communications-related services to that customer in any category of services.⁴ Customer permission does not allow the use or disclosure of customer information for any other purpose, including the marketing of non-communications-related services.⁵

duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of the call.

⁴ The "opt-out" permission system used by the Company does not extend to use of customer information for marketing by joint venture partners or independent contractors.

⁵ Except, of course, for those purposes for which customer permission is not required, as described above.

The Company utilizes an opt-out process for obtaining customer approval for use of customer information for marketing purposes. Under an opt-out permission system, the customer is provided with notice of the Company's intention to use his or her customer information in marketing communications related services to the customer. If the customer does not notify the Company within thirty-three days that he or she objects to (or opts-out of) this proposed use of customer information, permission to use the customer information will be assumed by the Company.

Customer opt-out permission is obtained as part of the Company Service Terms and Conditions documentation and as part of the documentation associated with customer service initiation. Opt-out permission may also be obtained or confirmed after service initiation through notice in a bill insert. Customers may revoke their opt-out permission at any time, and may do so either orally or in writing. The revocation need not be signed. Opt-out permission is valid for two years after the opt-out notice is sent, unless earlier revoked by the customer.

Records of customer permission of use or disclosure of customer information for marketing:

Customer records will be clearly marked as to whether permission for use or disclosure of customer information for marketing of communications related services has been granted. For customers whose records are not marked showing permission has been granted, the Company employees must assume permission has not been granted.

Approval and Recordkeeping for Use of Customer Information in a Marketing Campaign:

Before a supervisor may authorize employees to use customer information for marketing purposes, the proposed use of customer information must be reviewed and approved by the Company's counsel to assure the proposed use conforms with this policy and applicable federal regulations.⁶ Records of these reviews, including a description of the campaign, the specific customer information used in the campaign, and what products and services were offered as part of the campaign, will be maintained by marketing personnel.

Upon completion of a marketing campaign that uses customer information, or at regular intervals during the campaign, the appropriate supervisor will review the campaign to ensure the use of customer information is in accord with this policy. Copies of such evaluations will be sent to the designated marketing personnel for maintenance in the record of the campaign.

Employee Training: As part of initial orientation and training, all new employees will be provided training on Company policies and procedures with regard to protection and appropriate access and use of customer information. Training specific to each marketing campaign will be provided to employees at the initiation of any marketing campaign that uses customer information.

⁶ This requirement applies both to campaigns to market services in categories to which the customer already subscribes (i.e., campaigns that do not require customer permission) and to campaigns using opt-out permission to market communications-related services or communications services in categories to which the customer does not already subscribe.

SKP

Required Notifications and Annual Certification: To allow a customer to verify any change was intentional, the Company will notify a customer immediately, through telephone call to the customer's number of record or mail to the customer's address of record, of any changes to the customer's on-line account, address of record, password, or authentication questions established when the password was set up.

In any instance where a security breach results in customer information being disclosed to a third party without the customer's authorization, the employee discovering the breach must immediately notify the appropriate supervisor, who will notify the Company's counsel. Its counsel will, no later than seven days after determination of the breach, notify law enforcement through an online central reporting facility maintained by the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). Unless instructed otherwise by law enforcement, the Company will notify the customer of the breach seven days after reporting it to the USSS and FBI.

In any instance where the opt-out mechanism for customer approval for use of customer information in marketing does not work properly to such a degree that customers' inability to opt out is more than an anomaly, the appropriate supervisor must immediately notify the Company's counsel, which will provide the required notification to the Federal Communications Commission.

An appropriate officer of the Company will, by March 1st of each year, execute the required certification of the Company's compliance with customer information protection regulations along with the required report of actions taken against data brokers attempting to obtain customer information and summary of consumer complaints of unauthorized release of customer information during the previous calendar year.

Penalties for misuse or inappropriate disclosure of customer information; reporting misuse: Misuse or inappropriate disclosure of customer information can subject the Company to legal penalties that may include substantial monetary fines. Employees involved in misuse or inappropriate disclosure of customer information are subject to employee disciplinary action, including possible termination from employment.

Supervisors or employees aware of misuse or inappropriate disclosure of customer information must report that knowledge to the appropriate member of management when such misuse or inappropriate disclosure is discovered.